REMARKS

In the Official Action mailed on **22 December 2006**, the Examiner reviewed claims 1-27. The Oath and Declaration are defective. Claims 9, 18 and 27 were objected to because of informalities. Claims 7, 16 and 25 were rejected under 35 U.S.C. §112, second paragraph as being indefinite. Claims 10-18 were rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Claims 1-27 were rejected under 35 U.S.C. §102(e) as being anticipated by Immonen (US Pub. No. 2003/0120924 hereinafter "PGPub'924").

Objections to the Oath/Declaration

Examiner states that the oath or declaration is defective because it does not identify the country of residence of inventor Damien Bailly. Inventor Damien Bailly's country of residence is FRANCE. Applicant has enclosed a new Application Data Sheet, pursuant to MPEP 602.01, to overcome this problem.

Objections to the Claims

Claims 9, 18 and 27 were objected to because of informalities. More specifically, claims 9, 18 and 27 were objected to because the acronym (CBID) was not spelled out when first used in the claims. Applicant has amended claims 9, 18, and 27 to spell out CBID as "Crypto-Based Identifier." Support for this amendment can be found in paragraph **[004]** of the instant application.

Rejections under 35 U.S.C. §112

Claims 7, 16 and 25 were rejected under 35 U.S.C. §112, second paragraph as being indefinite. More specifically, claims 7, 16 and 25 were rejected because the claimed elements of "the sending device" and "the received GCA" do not have sufficient antecedent basis.

Claim 6, upon which claim 7 depends, recites the element of: "data received at the first device contains a cryptographically generated address (CGA) belonging to the second device." It is clear that "the received CGA" in claim 7 is referring to "the CGA" of claim 6, because the CGA of claim 6 is being received in the data from the second device. Applicant has amended claim 7 to remove the word "received" because it is unnecessary for the reason stated, and to conform to 35 U.S.C. §112. Furthermore, applicant has amended claim 7 to replace the term "sending" with the term "second" because it is also clear that the sending device is the second device.

Applicant has amended claims 16 and 25 in the same manner as claim 7, and for the same reasons. Support for these amendments can also be found in paragraphs **[009]** and **[0013]-[0014]** of the instant application.

Rejections under 35 U.S.C. §101

Claims 10-18 were rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Specifically, Claims 10-18 were rejected because paragraph **[0023]** of the instant application directs the computer-readable storage medium to include "computer instruction signals embodied in a transmission medium (with or without a carrier wave upon which the signals are modulated)." Applicant has amended paragraph **[0023]** to disavow the inclusion of "computer instruction signals embodied in a transmission medium" in a computer-readable storage medium.

Rejections under 35 U.S.C. §102(e)

Claims 1-27 were rejected under 35 U.S.C. §102(e) as being anticipated by PGPub'924. Applicant respectfully disagrees. Independent claims 1, 10, and 19 teach the benefit of "translating the data into a string of words that can be recognized by a human". This facilitates in allowing a user to confirm the data without having to perform the tedious task of comparing a long sequence of

numbers. For example, the instant application teaches an embodiment that translates a 128-bit address to a sequence of human-recognizable words using the One-Time Pass (OTP) dictionary (IETF RFC 1938) in which 11-bit numbers are mapped to human-recognizable words (paragraphs **[0026]** and **[0030]-[0031]** of the instant application).

In contrast, the cited reference does not suggest the importance of translating the data into a string of words that can be recognized by a human. Furthermore, the cited reference suggests, "advantageously, the check code is short, like 8 digits," (PGPub'924, paragraph **[0052]**, line 18). The cited reference teaches away from the use of long data strings which are potentially more secure, in favor of short check codes, which are potentially less secure.

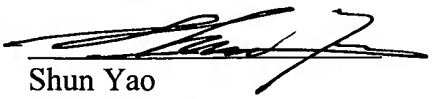
In regards to dependent claims 8, 17, and 26, Applicant contends that PGPub'924 does not suggest the use of the One-Time Pass (OTP) dictionary (IETF RFC 1938).

Hence, Applicant respectfully submits that independent claims 1, 10, and 19 as presently amended are in condition for allowance. Applicant also submits that claims 2-9, which depend upon claim 1, claims 11-18, which depend upon claim 10, and claims 20-27, which depend upon claim 19, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By 
Shun Yao
Registration No. 59,242

Date: 27 February 2007

Shun Yao
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1667
Fax: (530) 759-1665
Email: shun@parklegal.com